

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

Rec'd PCT/PTO

10 MAR 2005

(43) 国際公開日
2004年11月25日 (25.11.2004)

PCT

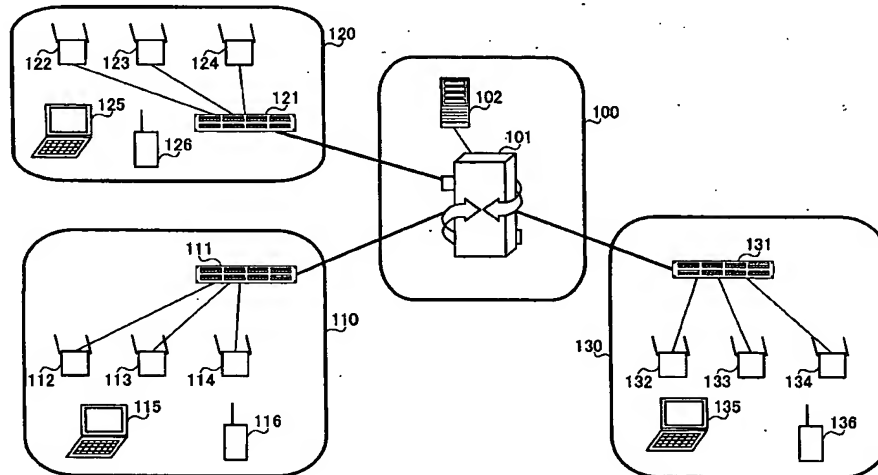
(10) 国際公開番号
WO 2004/102876 A1

- (51) 国際特許分類⁷: H04L 9/32, 9/08, 12/28, H04Q 7/38
- (21) 国際出願番号: PCT/JP2003/012125
- (22) 国際出願日: 2003年9月24日 (24.09.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2003-137830 2003年5月15日 (15.05.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 石井 義一 (ISHII, Yoshikazu) [JP/JP]; 〒227-0047 神奈川県横浜市青葉区みたけ台46-1-201 Kanagawa (JP).
- (74) 代理人: 鷺田 公一 (WASHIDA, Kimihito); 〒206-0034 東京都多摩市鶴牧1丁目24-1 新都市センタービル5階 Tokyo (JP).
- (81) 指定国 (国内): CN, KR, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).
- 添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: RADIO LAN ACCESS AUTHENTICATION SYSTEM

(54) 発明の名称: 無線LANアクセス認証システム



(57) Abstract: A radio LAN access authentication system capable of reducing the time required for an authentication process for accessing a radio terminal device. In this radio LAN access authentication system, when a radio terminal device (116) of a user where an access is requested is already registered by the initial access, a gateway device (111) searches a WEP key allocated to the radio terminal device (116) by a WEP key management section (306) and reallocates the WEP key registered in advance to a new access point section (124) as the shift destination and the radio terminal device (116). The radio terminal device (116) and the access point section (124) to which the WEP key is allocated perform communication while encrypting the transmission/reception data for a predetermined radio section by using the reallocated WEP key.

(57) 要約: 無線端末装置のアクセス認証の手続きに要する時間を短縮できるようにした無線LANアクセス認証システム。この無線LANアクセス認証システムにおいて、アクセス要求のあったユーザの無線端末装置116が、初期アクセスにより既に登録されている場合には、ゲートウェイ装置111がWEPキー管

[続葉有]



2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

理部306で無線端末装置116に割り当てられているWEPキーを検索し、予め登録されているWEPキーを移動先の新しいアクセスポイント部124及び無線端末装置116に再配布する。WEPキーを配布された無線端末装置116とアクセスポイント部124とは、再配布されたWEPキーを用いて所定の無線区間の送受信データを暗号化して通信を行う。

明 細 書

無線LANアクセス認証システム

5

技術分野

本発明は、無線信号を送受信する無線端末装置のアクセス認証を行う無線LANアクセス認証システムに関し、特に前記無線信号を伝送する無線区間を通して前記無線端末装置がアクセスする少なくとも2つ以上のアクセスポイント部を有する複数の無線LANネットワークシステムが統合されたネットワークシステムにおける無線LANアクセス認証システムに関する。

10

背景技術

近年のオフィス及び企業内などのローカルエリアネットワークシステム及び公衆ネットワークシステムにおいては、IEEE 802.11bなどの無線LAN規格を利用した無線LANネットワークシステムが運用されている。

15

このような無線LANネットワークシステムでは、ESSIDあるいはMACアドレスによる前記無線端末装置のアクセス認証及びWEP (Wired Equivalent Protocol) により前記無線区間を伝送される前記無線信号の暗号化が行われている。

20

しかしながら、このような前記無線端末装置のアクセス認証及び前記無線信号の暗号化は、セキュリティの脆弱性が指摘されている。このため、最近では、IEEE 802.1X (EAP: Extensible Authentication Protocol) を用いたRADIUS (Remote Authentication Dial-In User Service) サーバによる前記無線端末装置のアクセス認証及びWEPキーの動的な配布をサポートする機器による前記無線信号の暗号化を行うネットワークシステム

25

が構築されるようになってきている。

一方、このようなネットワークシステムの普及に伴って、前記ネットワークシステムを利用するユーザのより快適な通信を実現するために、複数のネットワークシステム間での前記無線端末装置のハンドオーバーの高速化が必要と
5 なっている。

このハンドオーバーの高速化を実現する従来の通信方式としては、前記ユーザの無線端末装置がハンドオーバーする可能性のあるアクセスポイント部において事前に前記無線端末装置のアクセス認証済み状態を作り、前記無線端末装置のハンドオーバー時の前記アクセスポイント部に対するアクセス認証を
10 不要として速やかな通信を行うようにした方式が提案されている（例えば、「2003年電子情報通信学会総合大会B-6-194「無線LANにおけるハンドオーバーの高速化に関する一考察」参照）。

この従来の通信方式では、次のような動作が実行される。

（1）この通信方式では、前記ユーザの無線端末装置の前記アクセスポイント部へのログイン時に、前記ユーザの無線端末装置と前記無線端末装置のアクセス認証を行う認証サーバ間とで通常のアクセス認証を行う。
15

（2）前記ユーザの無線端末装置がログインした前記アクセスポイント部と前記認証サーバとは、この後前記ユーザの無線端末装置が通信で用いる認証ヘッダとしてのアクセス認証時の証明書（セッションキー）を保持する。

（3）前記認証サーバは、予め保持している前記アクセスポイント部の地理的情報から前記ユーザの無線端末装置がハンドオーバーし得るアクセスポイント部を検索して該当するアクセスポイント部に前記セッションキーを配布する。
20

（4）前記ユーザの無線端末装置がハンドオーバーし得る周辺のアクセスポイント部は、前記認証サーバから通知された前記セッションキーを保持する。
25

（5）前記ユーザの無線端末装置と通信を行うアクセスポイント部は、前記無線端末装置がハンドオーバーを行った際に、前記アクセスポイント部が保持

している前記セッションキーと前記無線端末装置が保持しているセッションキーとの整合がとれていれば通信を許容する。

- (6) 前記ユーザの無線端末装置から初めてパケットの通信を検知したアクセスポイント部は、前記認証サーバに前記ユーザの無線端末装置のログインを
- 5 通知する。

(7) 前記認証サーバは、前記ユーザの無線端末装置が新たに入った通信エリアのアクセスポイント部へ前記セッションキーを通知し、前記通信エリア外に出たアクセスポイント部に対し前記セッションキーの解放を要求する。

- この通信方式においては、前記ユーザの無線端末装置がハンドオーバーする
- 10 可能性のある前記アクセスポイント部に対するアクセス認証が不要となり、前記無線端末装置と前記アクセスポイントとの速やかな通信が可能になる。

ところで、前記無線LANネットワークシステムとしては、例えば、企業内無線LANネットワークシステムと公衆無線LANネットワークシステムとを統合し、これらのネットワークシステム間を前記無線端末装置が移動する際

15 に、この無線端末装置の通信サービスをシームレスに継続するようなネットワークシステムが注目されつつある。このような複数の無線LANネットワークシステムを統合したネットワークシステムの形態としては、前記複数の無線LANネットワークシステムと交信するセンター局に前記認証サーバを配置して前記無線端末装置を集中的に管理するネットワークシステムが考えられる。

- 20 ここで、前記センター局で前記無線端末装置を集中管理する形態のネットワークシステムにおいて、前記無線端末装置が前記複数の無線LANネットワークシステム内を移動して新しいアクセスポイント部にハンドオーバーする場合について考える。

この場合、現状のIEEE 802.1Xを利用した無線LANアクセス認証

25 システムでは、前記無線端末装置がアクセスするアクセスポイント部が変わるたびに、前記無線端末装置と前記センター局の認証サーバとの間で認証番号(認証信号)の交換を行う必要がある。

このため、前記従来の無線LANアクセス認証システムにおいては、前記無線端末装置のアクセス認証及び前記無線区間を伝送される無線信号を暗号化するための暗号鍵であるWEPキーの配布に伴って行われるアクセス認証手続きにより前記無線端末装置のハンドオーバーに要する時間が増大してパケットロス招くという問題がある。

また、前記従来の無線LANアクセス認証システムでは、前記無線端末装置が複数のアクセスポイント部間を移動するたびに行われる前記無線端末装置と前記センター局との間での前記認証信号の交換のために、前記センター局と前記各無線LANネットワークシステムとの間の伝送路における前記認証信号などの制御信号の占有率が増大して、その伝送路帯域の有効利用が図れないという問題が発生する。

前述した通信方式（2003年電子情報通信学会総合大会B-6-194「無線LANにおけるハンドオーバーの高速化に関する一考察」参照）は、このような問題を解消しようとするものである。

しかしながら、前述したように、前記複数の無線LANネットワークシステムを統合し、前記無線端末装置のアクセス認証に用いるユーザID及び前記WEPキー等を前記センター局で一元管理しているような大規模なネットワークシステムでは、前記通信方式を適用することが困難となる。

すなわち、前記ユーザID及び前記WEPキー等が前記センター局で一元管理されている大規模なネットワークシステムに前記通信方式を適用した場合には、前記複数の無線LANネットワークシステム間を前記無線端末装置がシームレスに移動できるようにするために、前記無線端末装置が移動するたびに各無線LANネットワークシステムの周辺のアクセスポイント部に前記WEPキーの配布を行う必要がある。

このため、このような大規模なネットワークシステムでは、前記通信方式を取り入れても、前記センター局と前記複数の無線LANネットワークシステムの各々との間の伝送路を通して前記認証信号などの制御信号を頻繁に交換す

ることには変わりがない。

また、前記通信方式では、前記センター局の前記認証サーバが前記無線端末装置の位置情報及び前記無線LANネットワークシステムの各々のアクセスポイント部の地理的情報を管理する必要がある。しかし、このような各アクセスポイント部の地理的情報の管理を前記センター局の前記認証サーバが行うことは、前記認証サーバの負荷をさらに増大させることになる。

このようなことから、前述のように複数の無線LANネットワークシステムが統合された大規模のネットワークシステムでは、前記通信方式を適用することが非常に困難である。

10

発明の開示

本発明の目的は、複数の無線LANネットワークシステムを統合してセンター局で集中管理するネットワークシステムにおける無線端末装置のアクセス認証の手続きに要する時間を短縮でき、かつ前記センター局と前記無線LANネットワークシステムの各々との間の認証信号などの制御信号の数を低減することができる無線LANアクセス認証システムを提供することである。

前記目的を達成するために、本発明の無線LANアクセス認証システムは、複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と、前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置と、を有し、前記センター局は、前記複数の無線LANネットワークシステムの各々のゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置と、前記アクセスポイント部にアクセスされた前記無線端末装置のアクセス認証を行いアクセス認証された前記無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を前記無線端末装置及

20

25

- び前記アクセスポイント部に配布する認証サーバと、を有するネットワークシステムにおける無線LANアクセス認証システムであって、前記複数の無線LANネットワークシステムの各々に配設され自己の通信エリア内の前記無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に前記無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理手段と、前記複数の無線LANネットワークシステムの各々に配設され前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した前記無線端末装置が前記アクセス管理手段により前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理手段と、を具備する。
- 5
- 10

図面の簡単な説明

- 15 図1は、本発明の実施の形態1に係る無線LANアクセス認証システムの構成を示す概略構成図、
- 図2は、本発明の実施の形態1に係る無線LANアクセス認証システムにおけるアクセス認証の動作を示すシーケンス図、
- 図3は、本発明の実施の形態1に係る無線LANアクセス認証システムで使用する各無線LANネットワークシステムのゲートウェイ装置の構成を示す
- 20 ブロック図、
- 図4は、本発明の実施の形態1に係る無線LANアクセス認証システムにおいて無線端末装置が移動するときのアクセス認証の動作を示すシーケンス図、
- 図5は、本発明の実施の形態2に係る無線LANアクセス認証システムで使用する各無線LANネットワークシステムのゲートウェイ装置の構成を示す
- 25 ブロック図、
- 図6は、本発明の実施の形態2に係る無線LANアクセス認証システムにお

いて無線端末装置が移動するときのアクセス認証の動作を示すシーケンス図、

図7は、本発明の実施の形態3に係る無線LANアクセス認証システムに使用する無線端末装置の構成を示すブロック図、

図8は、本発明の実施の形態3に係る無線LANアクセス認証システムに使用する無線端末装置の他の構成を示すブロック図である。

発明を実施するための最良の形態

本発明の骨子は、複数の無線LANネットワークシステムを統合するセンター局の認証サーバへの無線端末装置のアクセス状況を各無線LANネットワークシステムのアクセス管理手段により管理し、新しいアクセスポイント部の通信エリアに移動した無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合に、無線区間の暗号鍵を各無線LANネットワークシステムの暗号鍵管理手段により前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布することである。

以下、本発明の実施の形態について、図面を参照して詳細に説明する。ただし、以下の説明では、前記無線LANネットワークシステムの例として、企業内無線LANネットワークシステムと公衆無線LANネットワークシステムとを統合したネットワークシステムを取り上げる。

(実施の形態1)

図1は、本発明の実施の形態1に係る無線LANアクセス認証システムを用いたネットワークシステムの構成を示す概略構成図である。図1に示すように、このネットワークシステムは、センター局100、本社内無線LANネットワークシステム110、支社内無線LANネットワークシステム120及び公衆無線LANネットワークシステム130を具備している。

図1において、センター局100は、本社内無線LANネットワークシステム110、支社内無線LANネットワークシステム120及び公衆無線LANネットワークシステム130を集中管理している。また、センター局100は、

センター局ゲートウェイ装置 101 及び認証サーバ 102 を有している。

一方、本社内無線 LAN ネットワークシステム 110 は、本社内ゲートウェイ装置 111 及び本社内アクセスポイント部 112、113、114 を有している。この本社内無線 LAN ネットワークシステム 110 では、ノートパソコン、PDA 及び携帯電話機などの無線端末装置 115、116 を用いて通信が行われる。

また、支社内無線 LAN ネットワークシステム 120 は、支社内ゲートウェイ装置 121、支社内アクセスポイント部 122、123、124 を有している。この支社内無線 LAN ネットワークシステム 120 では、ノートパソコン、PDA 及び携帯電話機などの無線端末装置 125、126 を用いて通信が行われる。

また、公衆無線 LAN ネットワークシステム 130 は、公衆ゲートウェイ装置 131、公衆アクセスポイント部 132、133、134 を有している。この公衆無線 LAN ネットワークシステム 130 では、ノートパソコン、PDA 及び携帯電話機などの無線端末装置 135、136 を用いて通信が行われる。

次いで、この実施の形態 1 に係る無線 LAN アクセス認証システムを用いたネットワークシステムの各構成装置の動作について、図 2 に示すシーケンス図を用いて説明する。

図 2 において、無線端末装置（ここでは、無線端末装置 116 とする）は、本社内無線 LAN ネットワークシステム 110、支社内無線 LAN ネットワークシステム 120 又は公衆無線 LAN ネットワークシステム 130 に初めてアクセスするときに、所望のアクセスポイント部（ここでは、本社内アクセスポイント部 114 とする）にアクセス要求を行う。この無線端末装置 116 は、無線区間を通して本社内アクセスポイント部 114 へのアクセスが完了した後、所定の認証手続きを経てアクセス認証される。

この認証手続きは、例えば、IEEE 802.1X のプロトコルに基づいて、無線端末装置 116 が、本社内無線 LAN ネットワークシステム 110 の本社

内ゲートウェイ装置 111 及びセンター局 100 のセンター局ゲートウェイ装置 101 を経由して、センター局 100 の認証サーバ 102 にアクセスすることで行われる。

- この認証手続きでは、図 2 に示すように、本社内アクセスポイント部 114
- 5 にアクセス要求を行った無線端末装置 116 に対して、本社内アクセスポイント部 114 から *Identity* が要求される。無線端末装置 116 は、前記 *Identity* の要求に対して、無線端末装置 116 のユーザのユーザ ID を含む応答信号を本社内アクセスポイント部 114 に送信する。前記応答信号を受信した本社内アクセスポイント部 114 は、無線端末装置 116 のアクセス認証を行うための認証信号を本社内ゲートウェイ装置 111 に送信する。
- 10

なお、ここでは、本社内無線 LAN ネットワークシステム 110 内の無線端末装置 116 が、本社内アクセスポイント部 114 を通してセンター局 100 の認証サーバ 102 にアクセスする場合について説明したが、他の無線端末装置についても同様に行われる。

- 15 本実施の形態 1 に係る無線 LAN アクセス認証システムを用いたネットワークシステムの各無線 LAN ネットワークシステム 110、120、130 に設置されるゲートウェイ装置 111、121、131 は、次のような構成を有している。

- 図 3 は、各ゲートウェイ装置 111、121、131 に共通した構成を有するゲートウェイ装置を示すブロック図である。
- 20

図 3 に示すように、ゲートウェイ装置 111、121、131 の各々は、データ送受信部 301、スイッチング部 302、スイッチング部 303、データ送受信部 304、ユーザアクセス管理部 305 及び WEP キー管理部 306 を備えている。

- 25 ここで、データ送受信部 301 は、交信するアクセスポイント部との間でデータの送受信を行う。スイッチング部 302 は、データ送受信部 301 に対する伝送路を選択する。スイッチング部 303 は、データ送受信部 304 に対す

る伝送路を選択する。データ送受信部 304 は、交信するセンター局ゲートウェイ装置との間でデータの送受信を行う。ユーザアクセス管理部 305 は、交信する各無線端末装置のアクセス状況を管理する。WEP キー管理部 306 は、割り当てられた無線端末装置と対応させて認証サーバ 102 より配布された

5 暗号鍵 (WEP キー) を管理する。

ゲートウェイ装置 (ここでは、本社内ゲートウェイ装置 111 とする) は、例えばアクセスポイント部 114 から送られてきた前記ユーザ ID を含む応答信号により、アクセス要求のあった無線端末装置 (ここでは、無線端末装置 116 とする) のアクセス状況を確認する。ここで、アクセス要求のあった無

10 線端末装置 116 が初めてアクセスする初期アクセスの無線端末装置である場合には、ユーザアクセス管理部 305 に「アクセスなし」と登録されている。

そして、この初期アクセスの場合には、ゲートウェイ装置 111 が、集中管理を行っているセンター局 100 のセンター局ゲートウェイ装置 101 を経由して、認証サーバ 102 に前記応答信号を転送する。

15 この応答信号を受信した認証サーバ 102 は、センター局ゲートウェイ装置 101、ゲートウェイ装置 111 及びアクセスポイント部 114 を経由して、アクセス要求のあった無線端末装置 116 との間で認証シーケンスの交換を行ってこのアクセス要求のあった無線端末装置 116 のアクセス認証を行う。

また、認証サーバ 102 は、前述のようにしてアクセス要求のあった無線端末装置 116 のアクセス認証が完了すると、この無線端末装置及び各アクセス
20 ポイント部に無線区間の送受信データを暗号化するための暗号鍵である WEP キーを配布する。このとき、ゲートウェイ装置 111 は、例えば、アクセス認証が完了した無線端末装置 116 のユーザ ID をユーザアクセス管理部 305 に登録して、アクセス認証が完了した無線端末装置 116 のアクセス状況
25 を管理する。

一方、WEP キー管理部 306 は、配布された前記暗号鍵 (WEP キー) と割り当てられた無線端末装置 116 とを対応させて、アクセス認証が完了した

無線端末装置 116 の WEP キーを保存する。前記 WEP キーを配布された無線端末装置 116 とアクセスポイント部 114 とは、前記 WEP キーを用いて前記無線区間の送受信データを暗号化して通信を行う。

次に、ある無線 LAN ネットワークシステムのアクセスポイント部を経由して通信を行っていた無線端末装置が、その移動により他の無線 LAN ネットワークシステムのアクセスポイント部を経由して通信するためのアクセス認証を行う場合の動作について説明する。

図 4 は、このようなアクセスポイント部間を移動する無線端末装置がアクセス認証を行う場合の動作を示すシーケンス図である。ここでは、前記無線 LAN ネットワークシステムを本社内無線 LAN ネットワークシステム 110 とし、前記アクセスポイント部を本社内アクセスポイント部 114 とする。また、前記無線端末装置を無線端末装置 116 とし、前記他の無線 LAN ネットワークシステムのアクセスポイント部を支社内無線 LAN ネットワークシステム 120 のアクセスポイント部 124 とする。

図 4 において、移動する無線端末装置 116 は、移動先の新たなアクセスポイント部 124 からビーコン（コールサイン及びキャリア）を検知し、この新たなアクセスポイント部 124 にアクセス要求を行って、所定の無線区間のアクセス手続きを行う。

この移動する無線端末装置 116 は、そのアクセス手続きが完了すると、そのアクセス認証を行うために新しいアクセスポイント部 124 から Identity の要求を受ける。この Identity の要求により、無線端末装置 116 は、ユーザ ID を含む応答信号を移動先の新たなアクセスポイント部 124 に送信する。

前記応答信号を受信したアクセスポイント部 124 は、無線端末装置 116 からの応答信号をゲートウェイ装置 121 に送信する。ゲートウェイ装置 121 は、アクセスポイント部 124 から送られてきた前記ユーザ ID を含む応答信号に基づいて、ユーザアクセス管理部 305 によりアクセス要求のあったユ

ーザの無線端末装置 116 のアクセス状況を確認する。

ここで、アクセス要求のあったユーザの無線端末装置 116 が、前述した初期アクセスにより既に登録されている場合には、ゲートウェイ装置 121 が、WE P キー管理部 306 でアクセス要求をしてきた無線端末装置 116 に割り当てられている WE P キーを検索し、予め登録されている WE P キーを移動先の新たなアクセスポイント部 124 及びアクセス要求のあった無線端末装置 116 に再配布する。

このようにして WE P キーを配布された無線端末装置 116 とアクセスポイント部 124 とは、再配布された前記 WE P キーを用いて所定の無線区間の送受信データを暗号化して通信を行う。

なお、ユーザアクセス管理部 305 及び WE P キー管理部 306 は、前記無線端末装置のアクセス状況及び割り当てられた WE P キーの管理を行うとともに、図示しないタイムアウト機能により、一定時間アクセス要求のない無線端末装置に対する登録を抹消して、前記無線端末装置の電源の OFF 及び他のドメインへの移動などにも対応する。

また、本実施の形態 1 に係る無線 LAN アクセス認証システムは、ゲートウェイ装置 111、121、131 の各々に、前記ユーザの無線端末装置のアクセス状況及び前記 WE P キーを管理するユーザアクセス管理部 305 及び WE P キー管理部 306 を配設する構成としたが、これらのユーザアクセス管理部 305 及び WE P キー管理部 306 は、前記ゲートウェイ装置から分離して、前記各無線 LAN ネットワークシステムに独立して配置した構成とすることも可能である。

このように、本実施の形態 1 に係る無線 LAN アクセス認証システムにおいては、前記無線端末装置が移動して新たなアクセスポイント部にアクセスする際のアクセス認証及び WE P キーの配布を、各無線 LAN ネットワークシステムに配置したゲートウェイ装置 111、121、131 で行うことができるので、前記無線端末装置の移動に伴うアクセス認証手続きに要する時間を短縮す

ることができる。

これにより、本実施の形態１に係る無線ＬＡＮアクセス認証システムにおいては、前記無線端末装置の移動時のハンドオーバーにかかる時間の短縮化及び各無線ＬＡＮネットワークシステムとセンター局１００との間の認証シグナ

５ リング数を大幅に低減して、伝送路の帯域の有効利用を実現することができる。

(実施の形態２)

次に、本発明の実施の形態２について、図面を参照して詳細に説明する。

本発明の実施の形態２に係る無線ＬＡＮアクセス認証システムは、本発明の実施の形態１に係る無線ＬＡＮアクセス認証システムの機能に加えて、交信す
10 る無線端末装置のアクセス時間及び通信パケット量をカウントする機能を有している。

この実施の形態２に係る無線ＬＡＮアクセス認証システムでは、交信する無線端末装置のアクセス時間もしくは通信パケット量が所定量に達した時点で、前記無線端末装置にセンター局１００の認証サーバ１０２との再認証及び新
15 しい暗号鍵の配布が要求される。

図５は、本実施の形態２に係る無線ＬＡＮアクセス認証システムで使用されるゲートウェイ装置の構成を示す。なお、この実施の形態２に係る無線ＬＡＮアクセス認証システムで使用されるゲートウェイ装置において、図３に示したゲートウェイ装置３００と同一の機能を有する構成要素には、同一符号を付し
20 てその詳細な説明を省略する。

図５に示すように、本実施の形態２に係る無線ＬＡＮアクセス認証システムで使用されるゲートウェイ装置５００は、本発明の実施の形態１におけるユーザアクセス管理部３０５の代わりにユーザアクセス管理部５０１を有している。このゲートウェイ装置５００のユーザアクセス管理部５０１は、アクセス
25 時間管理部５０２及び通信パケット量管理部５０３を備えている。アクセス時間管理部５０２は、交信している各無線端末装置のアクセス時間をカウントする。また、通信パケット量管理部５０３は、交信している各無線端末装置の通

信パケット量をカウントする。

次に、本実施の形態2に係る無線LANアクセス認証システムにおける無線
端末装置の再認証及び暗号鍵の再配布までの動作について説明する。図6は、
この実施の形態2に係る無線LANアクセス認証システムにおける無線端末
5 装置（ここでは、無線端末装置116とする）の再認証及び暗号鍵の再配布ま
での動作を示すシーケンス図である。

図6において、アクセス要求のあった無線端末装置116と認証サーバ10
2とのアクセス認証が完了すると、無線端末装置116が所望のネットワーク
システムとの通信を開始する。また、これと同時に、ゲートウェイ装置500
10 のアクセス時間管理部502及び通信パケット量管理部503が、無線端末装
置116のアクセス時間及びパケット量のカウントを開始する。

ここで、例えばアクセスポイント部114を経由して通信している無線端末
装置116が移動し、新たなアクセスポイント部124を経由して通信を行お
うとする場合には、ゲートウェイ装置500のWEPキー管理部306に管理
15 されている暗号鍵（WEPキー）が、この移動する無線端末装置116及び移
動先の新たなアクセスポイント部124に再配布される。これにより、この移
動する無線端末装置116は、その初期のアクセス認証時に配布された暗号鍵
と同じ暗号鍵を用いて通信が行われる。

その後、ゲートウェイ装置500のアクセス時間管理部502及び通信パケ
20 ット量管理部503によりカウントされたアクセス時間もしくは通信パケッ
ト量が所定量に達すると、ゲートウェイ装置500は、アクセスしている無線
端末装置116に対してセンター局100の認証サーバ102との間で再認
証と暗号鍵の再配布手続きを行うように要求信号を通知する。

このとき、ゲートウェイ装置500のユーザアクセス管理部501により管
25 理されているユーザの無線端末装置116のアクセス状況の登録内容は、前記
再認証が必要な状態であるという内容に変更される。また、この無線LANア
クセス認証システムの通信モードは、無線端末装置116から送られてくる認

証信号をセンター局100の認証サーバ102に転送するモードに切り換えられる。

これにより、前記再認証及び前記暗号鍵の再配布の要求信号を受け取った無線端末装置116が、アクセスポイント部124に認証要求信号を送信することにより、図6に示す一連の認証シーケンスが開始される。

そして、IEEE802.1Xのプロトコルに基づく所定の認証手続きが完了すると、新しい暗号鍵（WEPキー）が認証サーバ102より無線端末装置116と移動先の新たなアクセスポイント部124と配付され、無線端末装置116と移動先の新たなアクセスポイント部124とが新しい暗号鍵を用いて送信データの暗号化を行って通信を行う。

また、これと同時に、ゲートウェイ装置500は、WEPキー管理部306により新しい暗号鍵を保存し、アクセス時間管理部502及び通信パケット量管理部503により再び無線端末装置116のアクセス時間及びパケット量のカウンタを開始する。

このように、本実施の形態2に係る無線LANアクセス認証システムにおいては、ゲートウェイ装置500のアクセス時間管理部502及び通信パケット量管理部503により、無線端末装置116のアクセス時間及びパケット量が管理されている。

そして、アクセスしている無線端末装置116のアクセス時間及び通信パケット量が所定量に達した時点で、この無線端末装置116に、センター局100の認証サーバ102との間で、アクセス認証の再認証と暗号鍵の再配布との手続きを行うように要求される。

従って、本実施の形態2に係る無線LANアクセス認証システムによれば、アクセスしている無線端末装置のアクセス時間及び通信パケット量が所定量に達する毎に、この無線端末装置と前記無線端末装置のアクセスポイント部との間で使用される暗号鍵（WEPキー）が更新され、WEPキーの解読などによる不正な無線端末装置の成りすましアクセスを防止することができる。

(実施の形態3)

次に、本発明の実施の形態3について、図面を参照して詳細に説明する。

本発明の実施の形態3に係る無線LANアクセス認証システムは、前記各無線端末装置が、センター局100の認証サーバ102によりアクセス認証される際に用いるID情報が記録された情報カードとしてのSIM (Subscriber Identity Module) カードを搭載しており、このSIMカード内から前述のアクセス認証に用いるユーザIDを抽出してアクセス認証の手続きを行うものである。

図7は、本実施の形態3に係る無線LANアクセス認証システムで使用する無線端末装置の構成を示すブロック図である。図7に示すように、この無線端末装置700は、無線LAN I/F (無線LAN用のアクセスインターフェース) 701、SIMカード702、EAPクライアント703及びWEPクライアント704を備えている。

この無線端末装置700では、IEEE 802.1x (EAP: Extensible Authentication Protocol) 機能を有するEAPクライアント703が、センター局100の認証サーバ102との間で認証信号の交換を行う。そして、SIMカード702内に記録されているユーザIDを使用してIEEE 802.1xのシーケンスが遂行される。

なお、SIMカード702内に記録されているユーザIDは、センター局100の認証サーバ102にも登録されている。また、無線端末装置700は、WEPクライアント704により、アクセス認証後、認証サーバ102から付与された暗号鍵を用いて暗号化及び複合化を行う。

図8は、本実施の形態3に係る無線LANアクセス認証システムで使用する他の無線端末装置の構成を示すブロック図である。図8に示すように、この無線端末装置800は、図7に示した無線端末装置700の構成に加えて、セルラー無線 I/F 801及びセルラー認証クライアント802を備えている。すなわち、この無線端末装置800は、無線LAN用のアクセスインターフェー

スである無線LAN I/F 701に加えて、セルラー無線用のアクセスインターフェースであるセルラー無線 I/F 801を有している。

この無線端末装置 800では、図8に示すように、SIMカード 702に記録されたユーザIDがEAPクライアント 703に与えられて無線LANネットワークシステム側のアクセス認証に使用される。

また、この無線端末装置 800では、SIMカード 702に記録されたユーザIDがセルラー無線ネットワークシステム側の認証を行うセルラー認証クライアント 802にも与えられ、前記セルラー無線ネットワークシステム側のアクセス認証にも使用される。

10 なお、ここでは、無線端末装置 700または無線端末装置 800に搭載したSIMカード 702のユーザIDをアクセス認証に使用する例について説明したが、アクセス認証に使用するユーザ情報としては、例えば、第3世代携帯電話機に搭載されているUIM (User Identity Module) カードに記録されているユーザ情報を使用しても同様な認証手続きを行う
15 ことができる。

本実施の形態3に係る無線LANアクセス認証システムによれば、ユーザが無線端末装置の機種を変更した場合でも、このユーザのアクセス認証時の認証用IDが変更されてしまうことがなくなり、前記ユーザのユーザID及び前記ユーザへの課金を一元管理することができるほか、セルラー無線ネットワーク
20 システムと無線LANネットワークシステムとの両ネットワークシステムのアクセス認証及び課金に対しても一元化することができる。

本発明の一形態に係る無線LANアクセス認証システムは、複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と、前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置と、を有
25

し、前記センター局は、前記複数の無線LANネットワークシステムの各々のゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置と、前記アクセスポイント部にアクセスされた前記無線端末装置のアクセス認証を行いアクセス認証された前記無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を前記無線端末装置及び前記アクセスポイント部に配布する認証サーバと、を有するネットワークシステムにおける無線LANアクセス認証システムであって、前記複数の無線LANネットワークシステムの各々に配設され自己の通信エリア内の前記無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に前記無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理手段と、前記複数の無線LANネットワークシステムの各々に配設され前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した前記無線端末装置が前記アクセス管理手段により前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理手段と、を具備する構成を採る。

この構成においては、前記無線端末装置が所定の無線LANネットワーク内で移動した場合には、前記アクセス管理手段により前記無線端末装置の前記認証サーバへのアクセス状況が確認される。そして、この無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合には、前記暗号鍵管理手段により前記暗号鍵が前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布される。これにより、前記認証サーバに既にアクセスしていることが確認された前記無線端末装置は、前記新しいアクセスポイント部に移動する際に、前記センター局の前記認証サーバとの前記認証信号の交換を行うことなく、所望の無線LANネットワークへのアクセスが許可される。従って、この構成によれば、前記無線端末装置の移動に伴うアクセス

認証のための認証手続きに要する時間を短縮することができ、前記無線端末装置の前記新たなアクセスポイント部へのハンドオーバーを容易に行うことができ、前記各無線LANネットワークと前記センター局との間の認証信号などの制御信号の数（認証シグナリング数）を大幅に低減することができ、伝送路
5 の帯域の有効利用を実現することができる。

また、本発明の他の形態に係る無線LANアクセス認証システムは、前記アクセス管理手段及び前記暗号鍵管理手段が、前記ゲートウェイ装置に配設されている構成を採る。

この構成においては、前記アクセス管理手段及び前記暗号鍵管理手段が、前
10 記各無線LANネットワークの各ゲートウェイ装置に配設されているので、前記各無線LANネットワークの構成を簡素化することができる。

また、本発明のさらに他の形態に係る無線LANアクセス認証システムは、前記アクセス管理手段が、前記各無線端末装置のアクセス時間又は通信パケット量の少なくとも一方のアクセス量を管理し、前記アクセス量が所定量に達し
15 た時点で前記無線端末装置に再認証を要求する管理部を有する構成を採る。

この構成においては、前記アクセス量が所定量に達した時点で前記管理部より前記無線端末装置に再認証を要求することにより、この無線端末装置が通信する無線区間の暗号鍵を更新することが可能になる。従って、この構成によれば、前記暗号鍵の解読による不正無線端末装置の成りすましアクセスを防止す
20 ることができる。

また、本発明のさらに他の形態に係る無線LANアクセス認証システムは、前記無線端末装置がID情報を記録した情報カードを備えており、前記無線端末装置のアクセス認証時の認証用IDとして前記情報カードに記録されているID情報を用いる構成を採る。

25 この構成においては、前記無線端末装置の情報カード（例えば、SIMカード又はUIMカード）に記録されているID情報が、前記無線端末装置のアクセス認証時の認証用IDとして用いられる。従って、この構成によれば、ユー

ザが前記無線端末装置の機種を変更した場合でも、前記ユーザのアクセス認証時の認証用IDが変更されてしまうことがなく、ユーザID及び前記ユーザへの課金を一元管理することができる。

- また、本発明のさらに他の形態に係る無線LANアクセス認証方法は、複数
- 5 の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と、前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ
- 10 装置と、を有し、前記センター局は、前記複数の無線LANネットワークシステムの各々のゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置と、前記アクセスポイント部にアクセスされた前記無線端末装置のアクセス認証を行いアクセス認証された前記無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を前記無線端末装置及び前
- 15 記アクセスポイント部に配布する認証サーバと、を有するネットワークシステムにおける無線LANアクセス認証方法であって、前記各無線LANネットワークシステム内の無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に前記無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス
- 20 管理ステップと、前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した無線端末装置が前記アクセス管理ステップで前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理ステップ
- 25 と、を有するようにした。

この方法においては、前記無線端末装置が所定の無線LANネットワーク内で移動した場合には、前記アクセス管理ステップにおいて前記無線端末装置の

- 前記認証サーバへのアクセス状況が確認される。そして、前記無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合には、前記暗号鍵管理ステップにおいて前記暗号鍵が前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布される。これにより、前記認証サーバに既にアクセスしていることが確認された前記無線端末装置は、新しいアクセスポイント部に移動する際に、前記センター局の認証サーバとの認証信号の交換を行うことなく、所望の無線LANネットワークへのアクセスが許可される。従って、この構成によれば、前記無線端末装置の移動に伴うアクセス認証のための認証手続きに要する時間を短縮することができる。また、この構成によれば、前記無線端末装置の新たなアクセスポイント部へのハンドオーバーを容易に行うことができる。また、この構成によれば、前記各無線LANネットワークと前記センター局との間の認証信号などの制御信号の数（認証シグナリング数）を大幅に低減することができる。さらに、この構成によれば、伝送路の帯域の有効利用を実現することができる。
- 5 また、本発明のさらに他の形態に係る認証サーバは、複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と、前記各アクセスポイント部間の
- 10 データ信号及び制御信号の送受信を中継するゲートウェイ装置と、を有し、前記センター局は、前記複数の無線LANネットワークシステムの各々のゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置を有するネットワークシステムにおける無線LANアクセス認証システムにおいて前記無線端末装置のアクセス認証を行う前記センター局
- 15 に配置された認証サーバであって、前記各無線LANネットワークの所定のアクセスポイント部に前記無線端末装置がアクセスするときのアクセス認証を行うアクセス認証手段と、前記各無線LANネットワークの各ゲートウェイ装

置に対して前記無線端末装置がアクセスする無線区間の暗号鍵を一括して配布する暗号鍵配布手段と、を有する構成を採る。

この構成によれば、前記各無線端末装置のアクセス時のアクセス認証及び前記無線区間の暗号鍵の配布を一括して行うことができかつ前記各無線LAN

5 ネットワークの各ゲートウェイ装置に前記暗号鍵を配布することができる。

また、本発明のさらに他の形態に係るゲートウェイ装置は、複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部を有し、前記センター局は、前記複数の無線LANネットワークシステムの各々のゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置と、前記アクセスポイント部にアクセスされた前記無線端末装置のアクセス認証を行いアクセス認証された前記無線端末装置が通信する無線区間の暗号化に
10 用いる暗号鍵を前記無線端末装置及び前記アクセスポイント部に配布する認証サーバと、を有するネットワークシステムにおける無線LANアクセス認証システムにおける前記各無線LANネットワークのゲートウェイ装置であって、前記センター局のセンター局ゲートウェイ装置との前記データ信号及び前記制御信号の送受信を行う送受信手段と、前記各無線LANネットワーク内の
15 前記無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に前記無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理手段と、前記アクセス管理手段により前記認証サーバから配布される前記暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した前記無線端末装置が前記
20 認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の前記暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理手段と、を有す

る構成を採る。

この構成においては、前記ゲートウェイ装置のアクセス管理手段により、前記各無線LANネットワーク内の無線端末装置の前記認証サーバへのアクセス状況が管理される。前記アクセス管理手段は、前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に、この無線端末装置の前記認証サーバへのアクセスの有無を確認することができる。また、前記ゲートウェイ装置は、前記無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合に、前記暗号鍵管理手段により前記無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布することができる。従って、この構成によれば、前記無線端末装置の移動に伴う認証手続きに要する時間を短縮することができ、前記無線端末装置の新たなアクセスポイント部へのハンドオーバーを容易に行うことができ、前記各無線LANネットワークと前記センター局との間の認証シグナリング数を大幅に低減することができ、伝送路の帯域の有効利用を実現することができる。

また、本発明のさらに他の形態に係るゲートウェイ装置は、前記アクセス管理手段が、前記各無線端末装置のアクセス時間又は通信パケット量の少なくとも一方のアクセス量を管理し、前記アクセス量が所定量に達した時点で前記無線端末装置に再認証を要求する管理部を有する構成を採る。

この構成においては、前記アクセス量が所定量に達した時点で前記管理部より前記無線端末装置に再認証を要求して、この無線端末装置が通信する無線区間の暗号鍵を更新することが可能となる。従って、この構成によれば、前記暗号鍵の解読による不正無線端末装置の成りすましアクセスを防止することができる。

また、本発明のさらに他の形態に係る無線端末装置は、複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスす

る少なくとも2つ以上のアクセスポイント部と、前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置と、を有し、前記センター局は、前記複数の無線LANネットワークシステムの各々のゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置と、前記アクセスポイント部にアクセスされた前記無線端末装置のアクセス認証を行いアクセス認証された前記無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を前記無線端末装置及び前記アクセスポイント部に配布する認証サーバと、を有するネットワークシステムにおける無線LANアクセス認証システムにおいて使用される無線端末装置であって、前記センター局の前記認証サーバによりアクセス認証される際に用いるID情報が記録された情報カードを有する構成を採る。

この構成においては、前記無線端末装置の情報カード（例えば、SIMカード又はUIMカード）に記録されているID情報が、前記無線端末装置のアクセス認証時の認証用IDとして用いられる。従って、この構成によれば、ユーザが無線端末装置の機種を変更した場合でも、このユーザのアクセス認証時の認証用IDが変更されてしまうことがなくなり、ユーザID及びユーザへの課金を一元管理することができる。

本明細書は、2003年5月15日出願の特願2003-137830に基づく。この内容はすべてここに含めておく。

20 産業上の利用可能性

本発明は、無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部を有する複数の無線LANネットワークシステムが統合されたネットワークシステムにおける無線端末装置の無線LANアクセス認証システムに適用することができる。

請求の範囲

1. 複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、

- 5 前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と、前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置と、を有し、

- 前記センター局は、前記複数の無線LANネットワークシステムの各々のゲ
10 ートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局
ゲートウェイ装置と、前記アクセスポイント部にアクセスされた前記無線端末
装置のアクセス認証を行いアクセス認証された前記無線端末装置が通信する
無線区間の暗号化に用いる暗号鍵を前記無線端末装置及び前記アクセスポイ
ント部に配布する認証サーバと、を有するネットワークシステムにおける無線
15 LANアクセス認証システムであって、

- 前記複数の無線LANネットワークシステムの各々に配設され自己の通信
エリア内の前記無線端末装置の前記認証サーバへのアクセス状況を管理し前
記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に前
記無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管
20 理手段と、前記複数の無線LANネットワークシステムの各々に配設され前記
認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エ
リアに移動した前記無線端末装置が前記アクセス管理手段により前記認証サ
ーバに既にアクセスしていることが確認された場合に前記無線端末装置が通
信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先
25 の新たなアクセスポイント部に配布する暗号鍵管理手段と、を具備する無線L
ANアクセス認証システム。

2. 前記アクセス管理手段及び前記暗号鍵管理手段が、前記ゲートウェイ装

置に配設されている請求項1記載の無線LANアクセス認証システム。

3. 前記アクセス管理手段が、前記各無線端末装置のアクセス時間又は通信パケット量の少なくとも一方のアクセス量を管理し、前記アクセス量が所定量に達した時点で前記無線端末装置に再認証を要求する管理部を有する請求項

5 2記載の無線LANアクセス認証システム。

4. 前記無線端末装置がID情報を記録した情報カードを備えており、前記無線端末装置のアクセス認証時の認証用IDとして前記情報カードに記録されているID情報を用いる請求項1記載の無線LANアクセス認証システム。

5. 複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、

前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と、前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置と、を有し、

15 前記センター局は、前記複数の無線LANネットワークシステムの各々のゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置と、前記アクセスポイント部にアクセスされた前記無線端末装置のアクセス認証を行いアクセス認証された前記無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を前記無線端末装置及び前記アクセスポイント部に配布する認証サーバと、を有するネットワークシステムにおける無線

20 LANアクセス認証方法であって、

前記各無線LANネットワークシステム内の無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に前記無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理ステップと、前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した無線端末装置が前記アクセス管理ステップで前記認証サーバに既にアクセスしているこ

25

とが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理ステップと、を具備する無線LANアクセス認証方法。

6. 複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、

前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と、前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置と、を有し、

- 10 前記センター局は、前記複数の無線LANネットワークシステムの各々のゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置を有するネットワークシステムにおける無線LANアクセス認証システムにおいて前記無線端末装置のアクセス認証を行う前記センター局に配置された認証サーバであって、

- 15 前記各無線LANネットワークの所定のアクセスポイント部に前記無線端末装置がアクセスするときのアクセス認証を行うアクセス認証手段と、前記各無線LANネットワークの各ゲートウェイ装置に対して前記無線端末装置がアクセスする無線区間の暗号鍵を一括して配布する暗号鍵配布手段と、を有する認証サーバ。

- 20 7. 複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、

前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部を有し、

- 25 前記センター局は、前記複数の無線LANネットワークシステムの各々のゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置と、前記アクセスポイント部にアクセスされた前記無線端末

装置のアクセス認証を行いアクセス認証された前記無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を前記無線端末装置及び前記アクセスポイント部に配布する認証サーバと、を有するネットワークシステムにおける無線LANアクセス認証システムにおける前記各無線LANネットワークのゲートウェイ装置であって、

前記センター局のセンター局ゲートウェイ装置との前記データ信号及び前記制御信号の送受信を行う送受信手段と、前記各無線LANネットワーク内の前記無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に前記無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理手段と、前記アクセス管理手段により前記認証サーバから配布される前記暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した前記無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の前記暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理手段と、を有するゲートウェイ装置。

8. 前記アクセス管理手段が、前記各無線端末装置のアクセス時間又は通信パケット量の少なくとも一方のアクセス量を管理し、前記アクセス量が所定量に達した時点で前記無線端末装置に再認証を要求する管理部を有する請求項7記載のゲートウェイ装置。

9. 複数の無線LANネットワークシステムと前記複数の無線LANネットワークシステムを統合して管理するセンター局とを備え、

前記複数の無線LANネットワークシステムの各々は、無線信号を送受信する無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と、前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置と、を有し、

前記センター局は、前記複数の無線LANネットワークシステムの各々のゲ

- ートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置と、前記アクセスポイント部にアクセスされた前記無線端末装置のアクセス認証を行いアクセス認証された前記無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を前記無線端末装置及び前記アクセスポイント部に配布する認証サーバと、を有するネットワークシステムにおける無線LANアクセス認証システムにおいて使用される無線端末装置であって、
- 5 前記センター局の前記認証サーバによりアクセス認証される際に用いるID情報が記録された情報カードを有する無線端末装置。

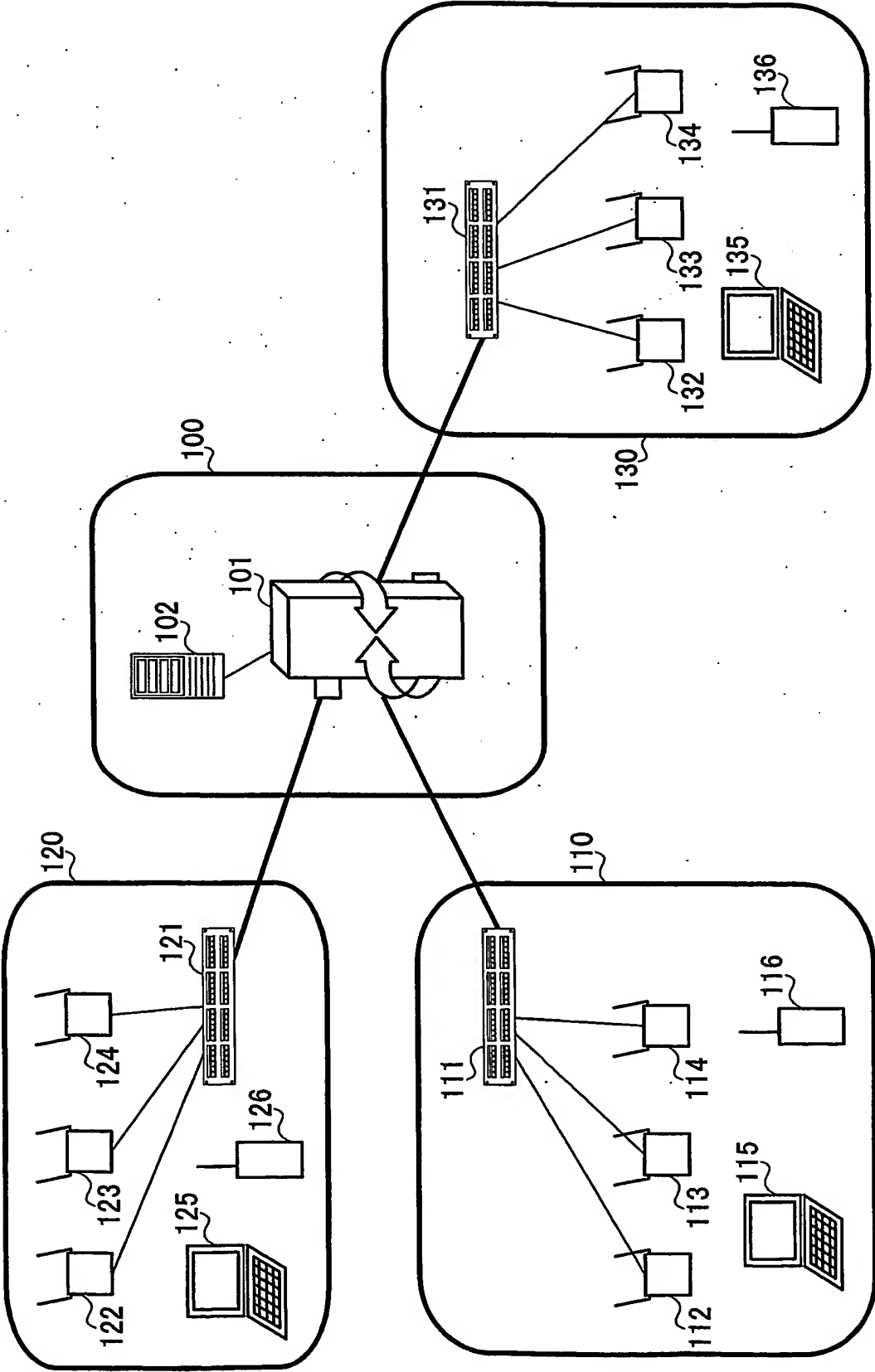


図 1

2/8

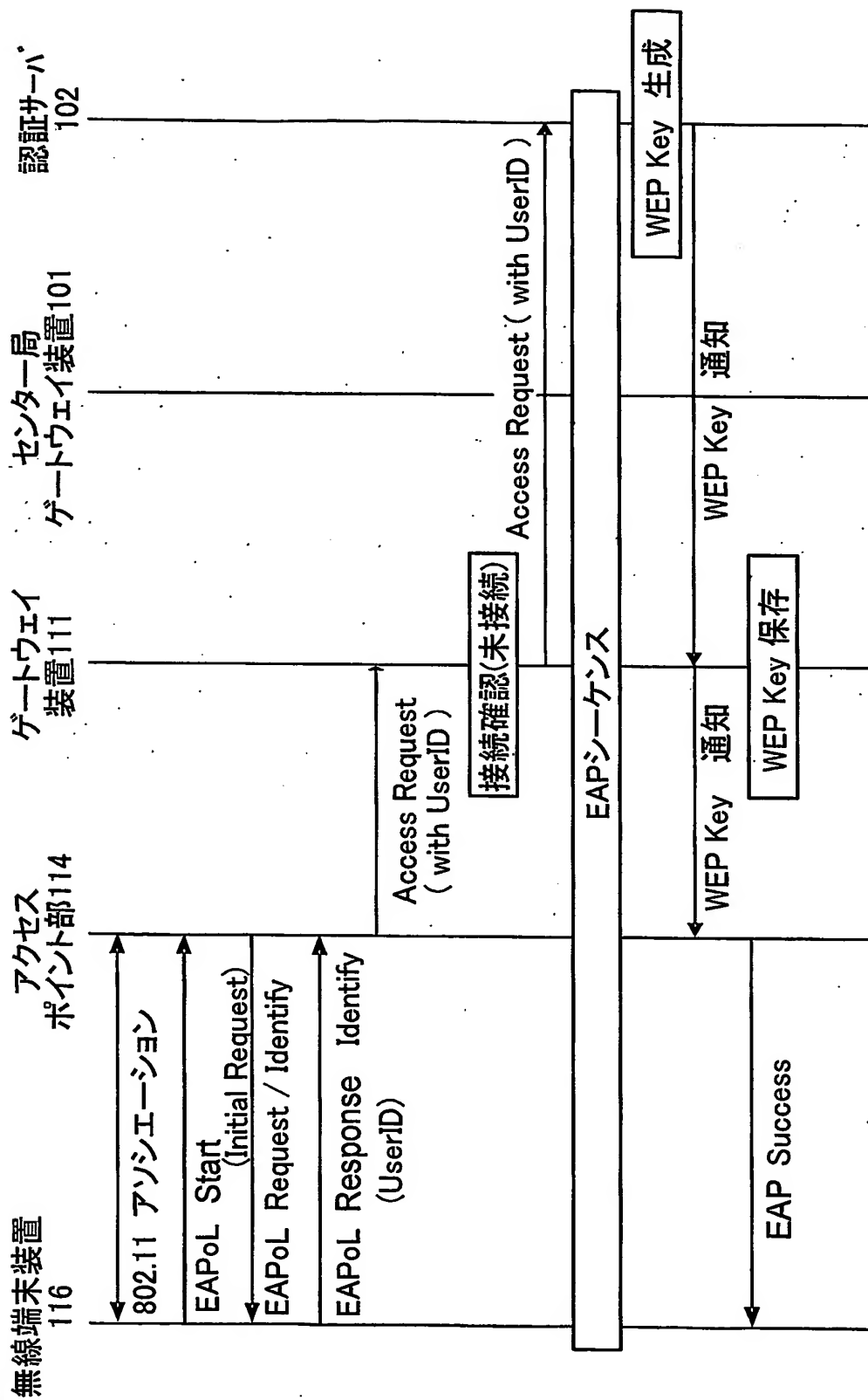


図 2

3/8

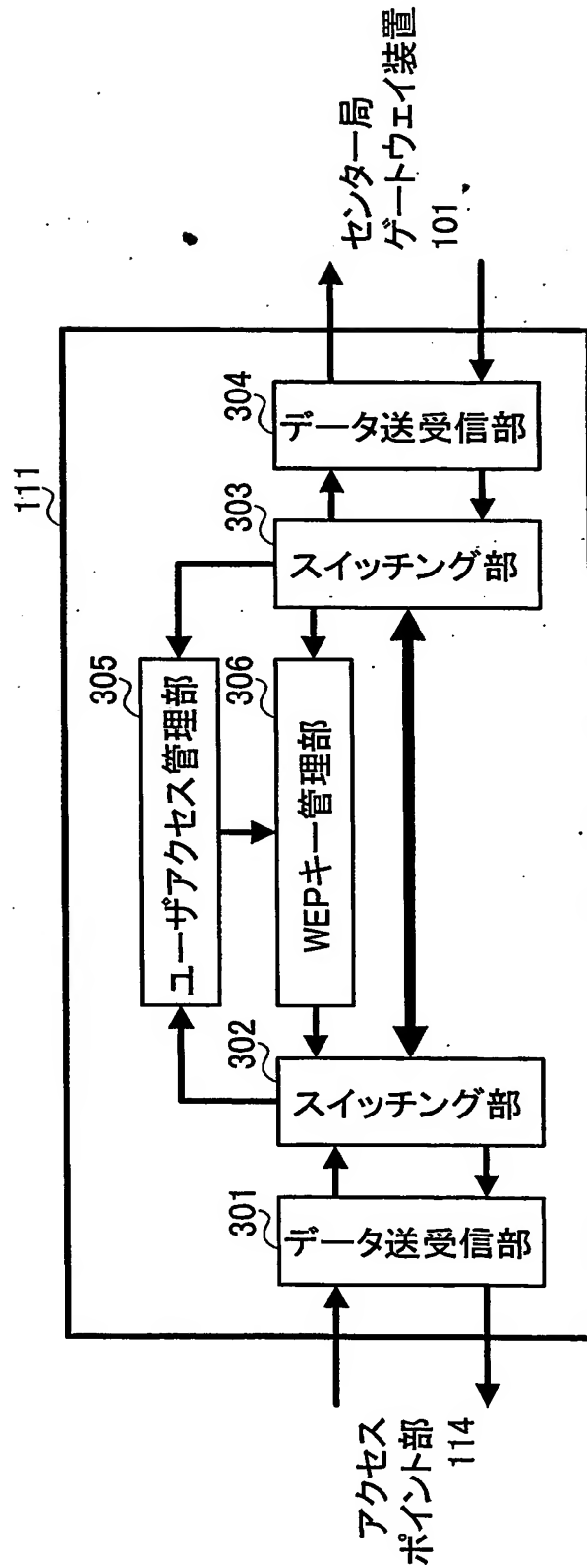


図 3

4/8

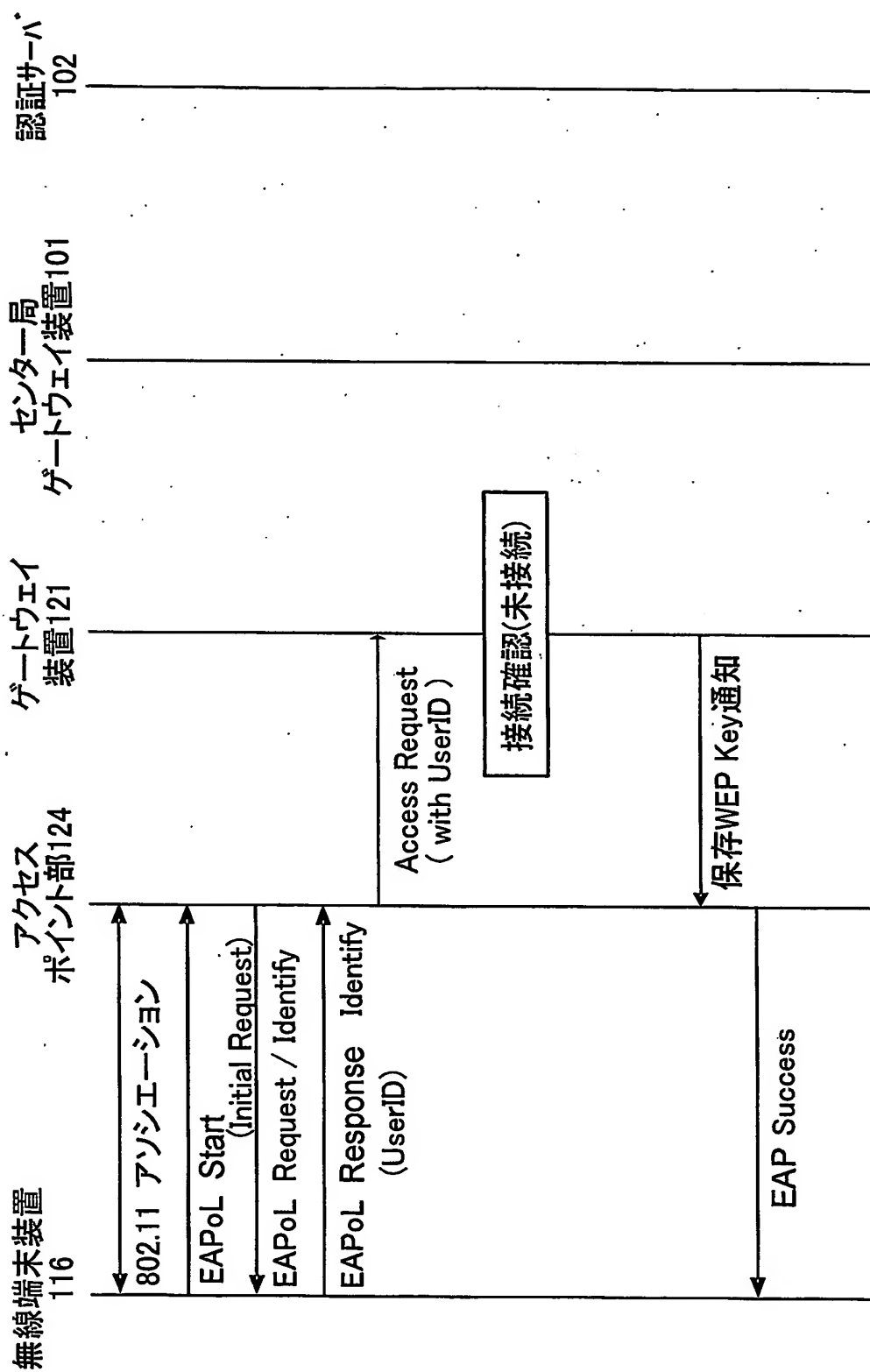


図 4

5/8

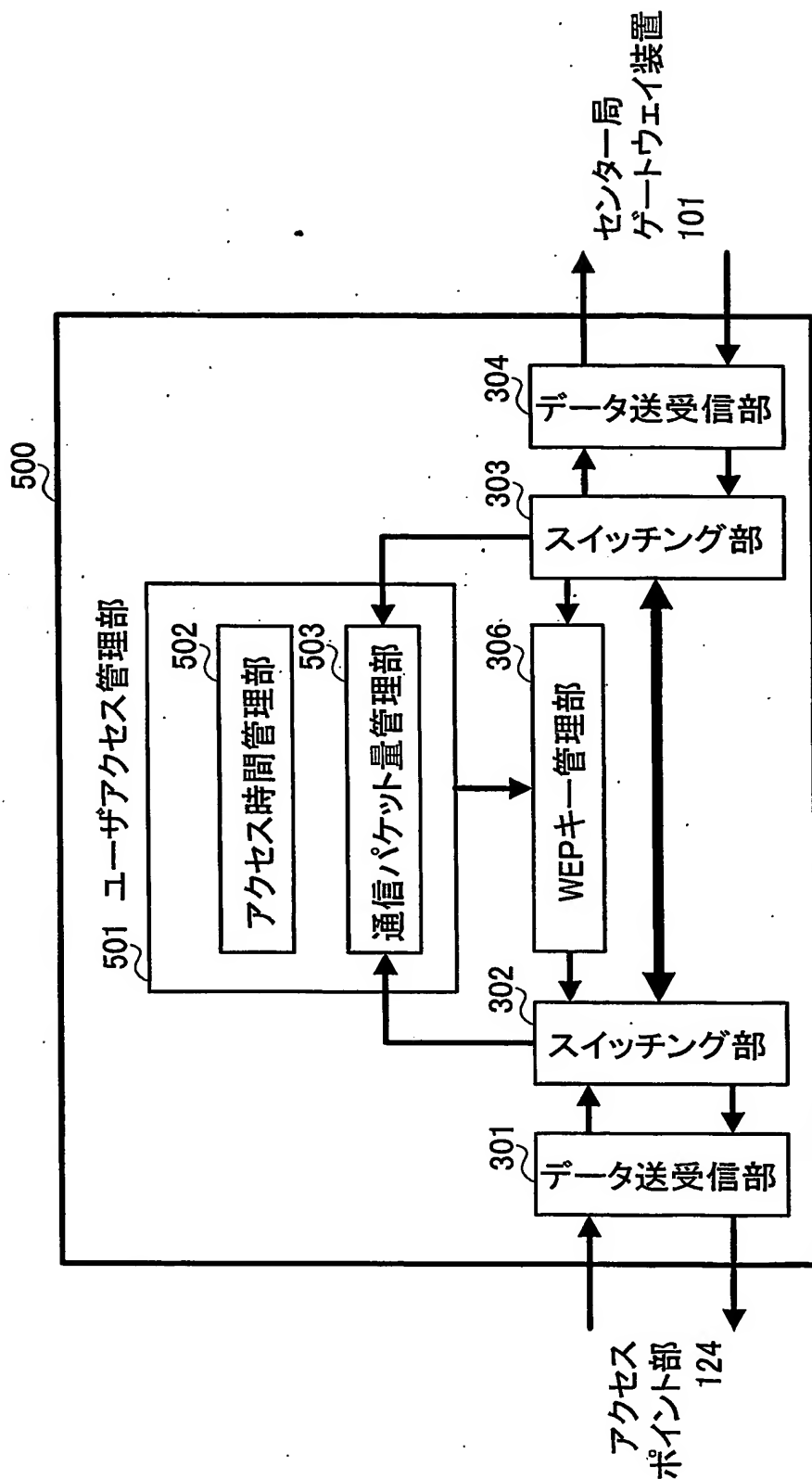


図 5

6/8

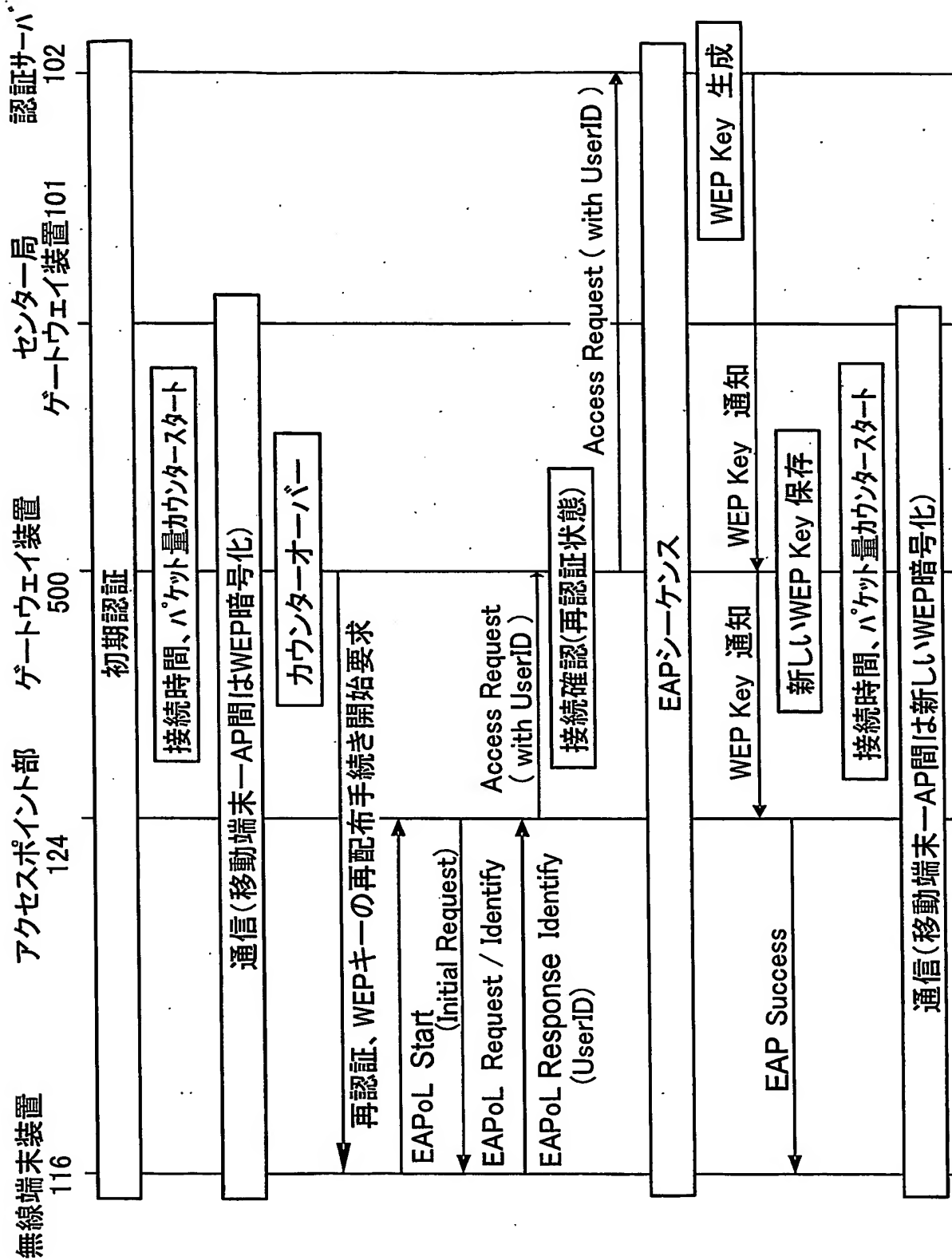


図 6

7/8

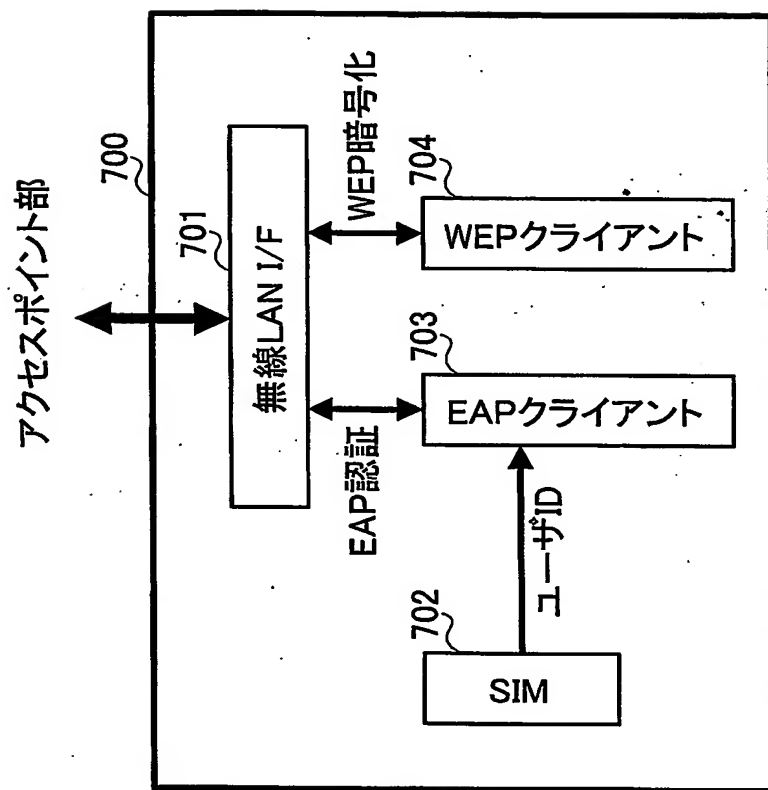


図 7

8/8

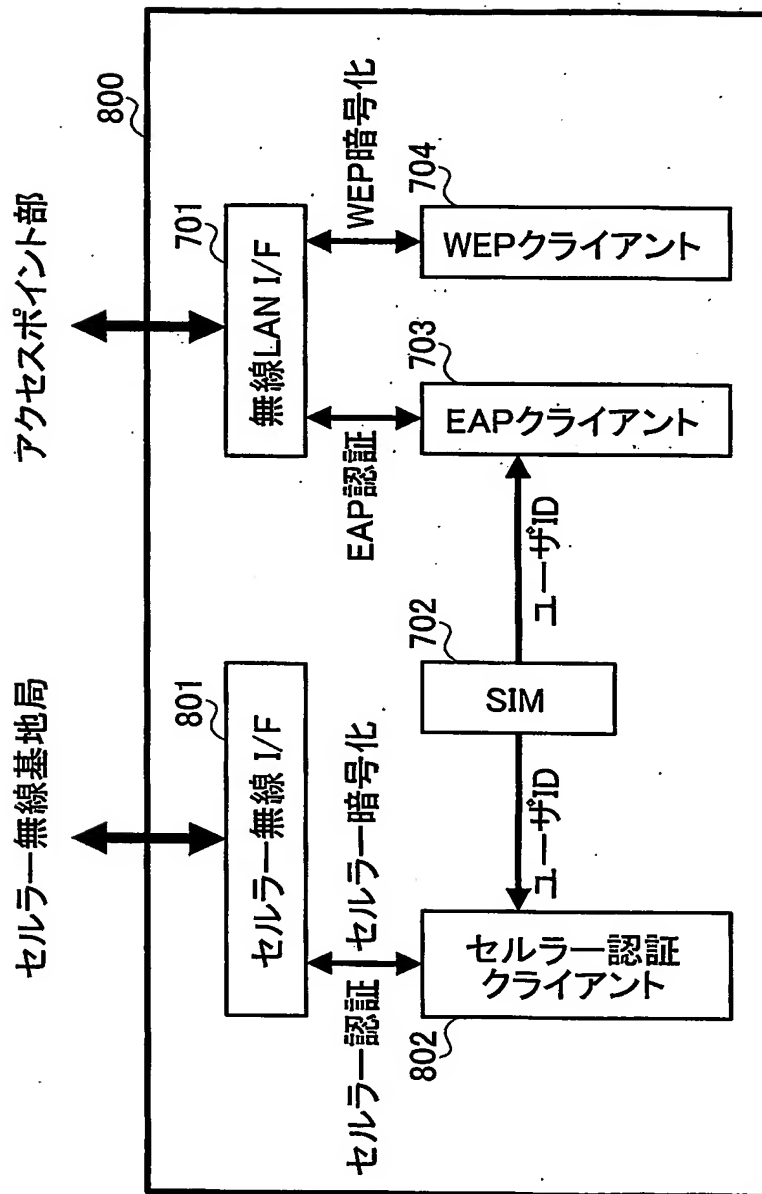


図 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/12125

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/32, H04L9/08, H04L12/28, H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/32, H04L9/08, H04L12/28, H04Q7/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 10-13956 A (NEC Corp.), 16 January, 1998 (16.01.98), Fig. 3 (Family: none)	1, 2, 4-7, 9 3, 8
Y A	JP 2002-118560 A (NTT Communications Kabushiki Kaisha), 19 April, 2002 (19.04.02), Full text (Family: none)	1, 2, 4-7, 9 3, 8
Y A	JP 2002-125270 A (Oki Electric Industry Co., Ltd.), 26 April, 2002 (26.04.02), Full text (Family: none)	1, 2, 4-7, 9 3, 8

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Date of the actual completion of the international search
17 December, 2003 (17.12.03)

Date of mailing of the international search report
13 January, 2004 (13.01.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/12125

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-300154 A (Toshiba Corp.), 11 October, 2002 (11.10.02), Fig. 3 (Family: none)	4, 9
Y	JP 5-183507 A (Nippon Telegraph And Telephone Corp.), 23 July, 1993 (23.07.93), Full text (Family: none)	4, 9
A	JP 2002-247047 A (The Furukawa Electric Co., Ltd.), 30 August, 2002 (30.08.02), Full text (Family: none)	1-9
A	JP 9-9349 A (NEC Tsushin System Kabushiki Kaisha), 10 January, 1997 (10.01.97), Full text (Family: none)	1-9
A	JP 11-225183 A (NTT Chuo Pasonaru Tsushinmo Kabushiki Kaisha), 17 August, 1999 (17.08.99), Full text (Family: none)	1-9

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/32, H04L9/08, H04L12/28, H04Q7/38

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/32, H04L9/08, H04L12/28, H04Q7/38

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2003年
 日本国登録実用新案公報 1994-2003年
 日本国実用新案登録公報 1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	JP 10-13956 A (日本電気株式会社) 1998. 01. 16, 第3図 (ファミリーなし)	1, 2, 4-7, 9 3, 8
Y A	JP 2002-118560 A (エヌ・ティ・ティ・コミュニケーションズ株式会社) 2002. 04. 19, 全文 (ファミリーなし)	1, 2, 4-7, 9 3, 8
Y A	JP 2002-125270 A (沖電気工業株式会社) 2002. 04. 26, 全文 (ファミリーなし)	1, 2, 4-7, 9 3, 8

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

17. 12. 03

国際調査報告の発送日

13.01.04

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石田 信行



5M

9469

電話番号 03-3581-1101 内線 3598

C (続き) . 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2002-300154 A (株式会社東芝) 2002. 10. 11, 第3図 (ファミリーなし)	4, 9
Y	JP 5-183507 A (日本電信電話株式会社) 1993. 07. 23, 全文 (ファミリーなし)	4, 9
A	JP 2002-247047 A (古河電気工業株式会社) 2002. 08. 30, 全文 (ファミリーなし)	1 - 9
A	JP 9-9349 A (日本電気通信システム株式会社) 1997. 01. 10, 全文 (ファミリーなし)	1 - 9
A	JP 11-225183 A (エヌ・ティ・ティ中央パーソナル通信網株式会社) 1999. 08. 17, 全文 (ファミリーなし)	1 - 9